

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

ŘÍZENÍ PŘÍSTUPU V SÍTÍCH IP

ACCESS CONTROL IN IP NETWORKS

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE

AUTHOR

Tomáš Frdlík

VEDOUCÍ PRÁCE

SUPERVISOR

prof. Ing. Ivan Baroňák, Ph.D.

BRNO 2018



Bakalářská práce

bakalářský studijní obor **Teleinformatika**

Ústav telekomunikací

Student: Tomáš Frdlík

ID: 164723

Ročník: 3

Akademický rok: 2017/18

NÁZEV TÉMATU:

Řízení přístupu v sítích IP

POKYNY PRO VYPRACOVÁNÍ:

Student v rámci bakalářské práce nastuduje problematiku kvality služeb (QoS) a problematiku metod AC (Admission Control). Dále se seznámí s problematikou neuronových sítí, navrhne a zdůvodní využití neuronových sítí pro potřebu AC metod s orientací na síť IP. Hlavní cílem práce je simulace AC metod a v prostředí IP sítí v programu MATLAB. Konkrétně se bude jednat o Gaussovu metodu a metodu využívající neuronové sítě. Výsledky simulace budou vhodně interpretovány a vzájemně porovnány (hlasový provoz pro více jak 100 zdrojů, 1 000 zdrojů, 10 000 zdrojů).

DOPORUČENÁ LITERATURA:

- [1] BRESLAU, L., JAMIN, S. and SHENKER, S.: Comments on the Performance of Measurement-Based Admission Control Algorithms. INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. 2000, pp. 1233-1242.
- [2] SHELDON M. ROSS: Introduction to Probability Models. University of California, Berkeley, USA, Eight Edition, ISBN 0-12-598055, 755 p.

Termín zadání: 18.6.2018

Termín odevzdání: 15.8.2018

Vedoucí práce: prof. Ing. Ivan Baroňák, Ph.D.

Konzultant:

prof. Ing. Jiří Mišurec, CSc.
předseda oborové rady

UPOZORNĚNÍ:

Autor bakalářské práce nesmí při vytváření bakalářské práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

Klíčová slova: AC metody, Gaussova metoda, neuronové sítě, metody řízení přístupu, QoS,

Abstrakt

V práci je popsána problematika zabezpečení QoS pro různé poskytované služby prostřednictvím IP sítí. Tyto aplikace mají vysoké nároky na parametry QoS jako zpoždění, ztrátovost a kolísání zpoždění.

Požadovanou kvalitu zabezpečujeme pomocí různých metod, které mají za úkol monitorování sítě a řízení provozu. Jedním z hlavních prvků QoS, kterému se v této práci věnujeme, jsou metody přístupové neboli AC metody. Tyto metody mají za úkol rozhodovat, zda přijmou nebo zamítnou nové spojení na základě jeho parametrů, aniž by ovlivnily QoS ostatních spojení. Dále se tato práce zabývá problematikou využití neuronových sítí v AC metodách. Na závěr práce jsou simulovány a porovnány dvě metody, Gaussova metoda a metoda s využitím neuronové sítě pro 100, 1 000 a 10 000 přístupů.

Keywords: AC methods, access control methods, Gaussian method, neuronové sítě, QoS.

Abstract

In this thesis we describe the problematic of QoS security for various services provided through IP network. These applications have high QoS parameter requirements such as delay, loss rate and variation of delay.

We provide the required quality using different methods that are responsible for network monitoring and traffic management. One of the main QoS elements we deal with in this thesis are AC methods. These methods have the task of deciding whether they accept or reject a new connection based on its parameters without affecting the QoS of other connections. Furthermore, this thesis deals with the use of neural networks in AC methods. At the end two methods are simulated and compared: the Gauss method and the neural network utilization method for 100, 1 000 and 10 000 accesses.

Bibliografická citace mé práce:

FRDLÍK, T. *Řízení přístupu v sítích IP*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2018. 46 s. Vedoucí bakalářské práce prof. Ing. Ivan Baroňák, Ph.D..

Prohlašuji, že svou bakalářskou práci na téma „Řízení přístupu v sítích IP“ jsem vypracoval samostatně, pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následku porušení ustanovení § 11 a následujících autorského zákona c. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku c. 40/2009 Sb.

V Brně dne podpis autora

Obsah

1	Úvod	8
2	Internet protokol	9
2.1	Služby poskytované v IP sítích.....	9
2.1.1	Přenos hlasu internetovým protokolem	9
2.1.2	Televizní přenos pomocí Internet protokolu.....	10
2.1.3	Přenos dat.....	10
3	kvalita služeb	11
3.1	Zabezpečení QoS	12
3.1.1	Model Best-Effort	12
3.1.2	Integrované služby	12
3.1.3	Diferencované služby	13
3.1.4	Metody řazení	13
3.2	Parametry kvality služeb.....	15
3.2.1	Zpoždění	16
3.2.2	Ztrátovost paketů	16
3.2.3	Rozptyl zpoždění	17
3.2.4	Přenosová kapacita	17
4	metody řízení přístupu	18
4.1	Difúzní metoda	20
4.2	Gaussova metoda	22
4.3	Další metody řízení přístupu.....	23

4.3.1	Metody řízení přístupu na základě měření.....	23
4.3.2	Metody řízení přístupu na základě parametrů.....	24
4.3.3	Algoritmus obyčejného sčítání	24
5	Neuronová síť	25
5.1	Neuron	26
5.2	Vícevrstvé neuronové sítě.....	27
5.2.1	Druhy vícevrstevných sítí.....	27
5.2.2	Adaptační algoritmus zpětného šíření chyby.....	28
5.3	Neuronové sítě v AC.....	29
6	Simulace a grafy	30
6.1	Grafy	31
6.1.1	Gaussova metoda	31
6.1.2	Metoda s neuronovou sítí.....	33
6.1.3	Porovnání	35
6.2	Vyhodnocení.....	37
7	Závěr	38
8	SEZNAM POUŽITÝCH ZKRATEK	39
9	SEZNAM POUŽITÝCH SYMBOLŮ	42
10	Seznam Použitých zdrojů	43

1 ÚVOD

V dnešní době existuje velké množství služeb poskytovaných přes internet zahrnující přenos hlasu přes internetový protokol (VoIP - Voice over Internet Protocol), Televizní vysílání pomocí Internet protokolu (IPTV - Internet Protocol Television), emaily, různé druhy streamů a chatů v reálném čase, přenosy velkého množství dat, cloudové služby a například i hromadně hrané online hry (MMO - Massively Multiplayer Online). Vzhledem k současnému nárůstu využívání internetových služeb i požadavky na šířku pásma stále stoupají. Šířka pásma je však limitována a to jak technologicky tak svou dostupností. Dnešní vysoké nároky na šířku pásma datových sítí mohou snadno přesáhnout jejich kapacitu. Tím dochází k zahlcení sítě následnému zpoždění a po čase i ztrátě paketů, což je značně nežádoucí. Jako řešení tohoto problému byla implementována služba pro zajištění kvality služeb (QoS - Quality of Service). Hlavním úkolem QoS je monitorování a následné řízení datového toku sítí pro efektivnější využívání daného přenosové kapacity linky. To vede k potlačení negativních jevů jako je výše zmíněné zpoždění nebo dokonce ztráta dat při přenosu. Metod využívaných QoS je mnoho, a to už jak metody řídící provoz tak rozdělení přenosové kapacity linky. Tato práce je zaměřena na konkrétní metody a to metody přístupové (AC - Admission Control).

Úkolem tohoto souboru metod je rozhodování, zda bude další spojení navázáno či nikoliv. A to tím způsobem, že na základě různých algoritmů, měření a odhadů zjistí, zda má linka dostatečnou kapacitu pro nové připojení, aniž by zhoršilo QoS již existujících připojení. Právě díky případnému odmítnutí dalších spojení, které by překračovaly kapacitu sítě, tyto metody zabraňují nežádoucímu zahlcení.

2 INTERNET PROTOKOL

Internet protokol (IP - Internet protocol) je základní komunikační datagramový protokol určený k přenosu a směrování dat v sítích. Je schopen adresovat a dále pak směrovat pakety od odesílatele k příjemci přes jednu či několik sítí. Každý z těchto paketů se skládá ze dvou částí: hlavičky a datové části. Hlavička je složena z řídících dat, mezi něž patří cílová adresa, počáteční adresa, číslo portu, případně označení aplikace. Datová část obsahuje přenášená data. Nejvíce rozšířená verze IP protokolu je IPv4 ačkoliv je v posledních letech nahrazována novou verzí IPv6, a to především z důvodu nedostatečné adresní kapacity. IPv4 může poskytnout pouze 2^{32} adres (což je něco přes 4 miliardy) zatímco IPv6 nabízí adresní prostor o velikosti 2^{128} adres [1].

2.1 Služby poskytované v IP sítích

2.1.1 Přenos hlasu internetovým protokolem

Přenos hlasu internetovým protokolem (VoIP – Voice over Internet Protocol) je služba, která zahrnuje množství technologií k přenosu hlasové komunikace a multimediálních relací prostřednictvím IP sítí. Vzhledem k tomu že služba VoIP je poskytována stejnou sítí jako ostatní datové služby, je důležité pro ni zabezpečit určitou kvalitu datového přenosu. Tuto kvalitu ovlivňuje velké množství faktorů jako například: ztrátovost paketů, zpoždění, rozptyl zpoždění, typ kodeků nebo paktizace.

Oproti většině aplikací používajících protokol řízení provozu (TCP - Transmission Control Protocol), VoIP využívá protokoly pro transport v reálném čase (RTP - Real-time Transport Protocol), uživatelský datagramový protokol (UDP - User Datagram Protocol) a IP protokol. Je tomu tak proto, že ačkoli je TCP spolehlivý transportní protokol, využívá ke spolehlivému přenosu potvrzení o doručení a případné znovuslání paketů. Toto potvrzování a případné znovuslání paketů způsobuje značné zpoždění, které není pro službu VoIP vhodné. Oproti tomu UDP využívá ne příliš spolehlivý IP protokol na přenos zpráv mezi koncovými uživateli. UDP ve spojení s RTP zajišťuje přenos dat, jako například hlas nebo video, v reálném čase. RTP nezaručuje bezchybný přenos ani QoS jako TCP. Proto se pro monitorování a řízení linky používá řídicí protokol pro transport v reálném čase (RTCP - Real-time Transport Control

Protocol).

Ztrátovost paketů služby VoIP menší než 2% je stále přijatelná, mezi 2-5% už je znatelný šum a hovor může být nesrozumitelný, nad 10% je již ztrátovost příliš vysoká. Zpoždění jednotlivých paketů by se mělo pohybovat maximálně mezi 150-400ms, u vyššího zpoždění je hlasový přenos považován za nefunkční. Kolísání zpoždění by nemělo překročit 40ms, je řešeno použitím vyrovnávacích pamětí u každého příjemce, což ale zvyšuje vnímané zpoždění [5], [3].

2.1.2 Televizní přenos pomocí Internet protokolu

Televizní přenos pomocí IP (IPTV – Internet protocol television) poskytuje službu digitální televize přes IP protokol. IPTV služba zahrnuje tři prvky: hromadné televizní vysílání, video na vyžádání (VoD – Video on Demand) a digitální videorekordér (DVR – Digital Video Recorder). Požadavky na QoS závisí zejména na použitých audio a video kodecích. Různé kodeky využívajících různou šířku pásma pro přenos, je tedy nutné vyhradit dostatečnou šířku pásma pro daný kodek. Pro kvalitní přenos je třeba ztrátovost a chybovost paketů menší než 1%, zpoždění do 200ms a kolísání zpoždění (jitter) maximálně 50ms [2].

2.1.3 Přenos dat

U přenosu dat je kladen hlavně důraz na to, aby data byla přenesena bez chyb. Proto je vyžadována co nejnížší ztrátovost paketů, pokud možno nulová. K přenosu tohoto typu se většinou využívá spojově orientovaného protokolu TCP, který v případě ztráty nebo poškození přenášených dat zažádá o opětovné zaslání. Zpoždění ani jeho kolísání není pro přenos dat příliš důležitý parametr [3].

3 KVALITA SLUŽEB

Kvalita služeb (QoS – Quality of Service) je souhrn mechanismů, které mají za úkol spravovat přetížený síťový provoz. Toto přetížení je způsobeno, když požadavek na zdroje překročí celkovou dostupnou kapacitu sítě. Jsou zde síťová omezení, kterým se nelze vyhnout, jako například technologické omezení, cena nebo dostupnost širokopásmových služeb. Šířka pásma definuje, jakou přenosovou kapacitu má síť. Pokud v síti probíhá větší množství komunikace, je zapotřebí větší přenosová kapacita. Často dochází k tomu, že požadavky na síť jsou vyšší než co je schopna přenést. V takovém případě zařízení pozastaví komunikaci, uloží si vysílané pakety do paměti a čeká, než bude mít prostředky, k jejich poslání. Tímto pozastavením komunikace dochází ke zpoždění. Pokud se počet vysílaných paketů stále nesnižuje, může dojít k situaci, kdy zařízení už není schopné další pakety ukládat do paměti a dojde k zahazování náhodných paketů. Aby takto nedocházelo ke ztrátě důležitých paketů, používají se QoS mechanismy. Ty stanoví prioritu různých druhů komunikace. Některé druhy komunikace nejsou tolik náchylné na zpoždění, u jiných je zase důležitá, aby byla ztrátovost co nejnižší. Právě podle těchto priorit jim QoS mechanismy přiřadí potřebné síťové zdroje, aby data byla doručena co nejefektivněji. Díky této možnosti třídění je možné zajistit potřebné QoS pro klíčové aplikace a efektivně využívat síťové zdroje [8].

3.1 Zabezpečení QoS

Základním úkolem QoS je poskytnout jistou úroveň služeb, kterou jednotlivé aplikace požadují a to tak, aby tím nebyla negativně ovlivněna úroveň služeb další aplikací. Avšak zajistit takovouto úroveň služeb v IP sítích je poměrně náročné protože neexistuje jednotná definice pojmu QoS. Je to způsobeno tím, že požadavky jednotlivých aplikací se liší. A to jak typem aplikace, síťovým rozhraním tak i požadavky samotného uživatele.

QoS můžeme rozdělit do třech základních skupin v závislosti na použitých mechanismech a to:

- Negarantované služby (BES - Best-Effort Service).
- Integrované služby (Interserv - Integrated Service),
- Diferenciované služby (Diffserv - Differentiated Services).

3.1.1 Model Best-Effort

Best-Effort je základní model, ve kterém se přidělování kapacit neřídí žádným systematickým postupem. Směrovač se snaží o to, aby všem aplikacím přidělil stejné kapacity a neupřednostňoval tím nějaké aplikace před jinými. Pokud požadavky na přenos dat přesahují přidělenou kapacitu, jsou zařazeny do fronty a následně, pokud nejsou odeslány, jsou náhodně zahazovány. Tento způsob negativně působí na celkové QoS a mohou nastávat výpadky v přenosu dat [9].

3.1.2 Integrované služby

Pokud využíváme model Integrované služby (IntServ – Integrated Services), musí každá aplikace před začátkem komunikace oznámit síti své požadavky na parametry přenosu. Například jakou minimální přenosovou kapacitu bude využívat, jaké maximální zpoždění je přijatelné a jaký vysoká může být ztrátovost paketů.

Následně síť ověří, jestli může těmto parametrům vyhovět a rozhodne, zda naváže nebo nenaváže spojení. Pokud spojení naváže, informuje o tom komponenty sítě podílející se na přenosu pomocí protokolu rezervace síťových prostředků (RSVP –

Resource reSerVation Protocol). Tyto komponenty následně musejí zajistit požadované parametry přenosu, čímž zabezpečí odpovídající úroveň QoS. [9]

3.1.3 Diferencované služby

Posledním druhem zabezpečení QoS jsou diferencované služby (DiffServ – Differentiated Services). V současnosti se trend ubírá právě směrem k používání tohoto modelu. Oproti IntServ se požadavky na parametry přenosu neoznamují před navázáním spojení. Tím pádem si jednotlivé síťové komponenty nemusí držet stavové informace o různých přenosech. Místo toho jsou pakety jednotlivých služeb označovány tak, aby bylo jasné definované, jak se má s daným paketem zacházet. Toto klasifikování přenosů a následné značkování paketů se uskutečňuje pouze na hraničních směrovačích a při průchodu dalšími síťovými prvky jsou tyto značky pouze čteny a následně podle nich přiřazovány do front. Tato značka se u paketu ukládá do pole typu služby (TOS - type of service) pro verzi IPv4 a do pole třídy provozu (TC - Traffic Class) pro verzi IPv6 [9].

3.1.4 Metody řazení

I. Metoda řazení paketů „první dovnitř, první ven“

Metoda řazení paketů „první dovnitř, první ven“ je základní metoda řazení paketů. Pakety jsou řazeny do jediné fronty a následně zpracovány ve stejném pořadí jako do uzlu dorazily. Tato metoda je velmi jednoduchá, avšak ne příliš vhodná pro sítě využívající aplikace s velkými požadavky na přenosové zdroje [9], [10].

II. Metoda řazení na základě váhy

Jedna z nejvíce používaných metod řazení paketu ve směrovačích je metoda řazení na základě váhy paketu (WFQ – Weight Fair Queuing). Využívá řazení do více front v závislosti na původu dat. Následně jsou pakety z těchto front zpracovány a jsou jim přidělena dostupné přenosové kapacity linky. Tímto postupem metoda zabraňuje situaci, kdy jedna aplikace spotřebuje příliš velkou část přenosové kapacity [9], [10].

III. Metoda prioritního řazení

Metoda prioritního řazení (PQ – Priority Queuing) zajišťuje prioritní zpracování datové toku, který je pro daný typ sítě důležitý. Metoda rozděluje datové toky do front s různou prioritou. Ty jsou následně, dle úrovně priority, zpracovány od nejdůležitější po nejméně důležité. Pokud není daná úroveň priority prázdná, nejsou zpracovány data z nižších úrovní priority. Tato metoda je vhodná pro sítě s důležitou komunikací. Avšak v případě přenosu příliš velkého množství dat s vysokou prioritou může dojít k zahlcení paměti pro fronty s nižším stupněm priority a tím ke zhoršení kvality ostatních poskytovaných služeb [9], [10].

IV. Metoda řazení podle vlastních požadavků

Metoda řazení podle vlastních požadavků (CQ – Custom Queuing) umožňuje přímo ovlivňovat a měnit procentuální poměr přiřazovaných přenosových kapacit pro jednotlivé aplikace. Pokud aplikace nevyužívá toto pásmo, pak je možné jej využívat pro jiný druh aplikace. Tato metoda je určena pro sítě, kde je potřeba zajistit kvalitu služby pro více typu přenosů. Aplikace lze identifikovat například podle využívaných portů [9], [10].

V. Metoda PQ/WFQ

Tato metoda je kombinací metod PQ a WFQ, avšak fronta PQ zde má před frontou WFQ absolutní prioritu. Tím docílíme, že při vyprázdňení prioritní fronty budou ostatní fronty s nižší prioritou obslouženy rovnoměrně a některé typy komunikace tak nebudou úplně pozastaveny, jako to bylo u metody PQ [9], [10].

VI. Metoda CB/WFQ

Kombinace metod CB a WFQ. Umožní rozdělení komunikace až na 64 front v závislosti na označení, které je jim přiřazeno v metodě DiffServ. Pro každou frontu pak lze přiřadit relativní nebo absolutní přenosovou kapacitu. Pokud označení pro danou komunikaci neodpovídá žádnému z kritérií, je přiřazena do základní fronty a následně zařazena pomocí metody WFQ. Pomocí této metody je možno některé druhy komunikace priorizovat před ostatními a přiřadit jim požadovanou přenosovou kapacitu [9], [10].

VII. Metoda řazení paketů s nízkým zpožděním

Metoda řazení paketů s nízkým zpožděním (LLQ – Low Latency Queuing) je rozšířením metody CB/WFQ které je zaměřena na priorizaci určitých datových toků a minimalizaci zpoždění. Tato metoda pracuje tím způsobem, že je jedna či více front prioritních a ty jsou obsluhovány, dokud v nich jsou pakety. Tento princip je podobný metodě PQ, avšak liší se od ní tím, že méně priorizované toky nejsou úplně zastaveny. Tokům s vysokou prioritou je přiřazena maximální přenosová kapacita. Pokud je tato hraniční šířka překročena, jsou pakety ve frontě zahozeny. Proto by se tato přenosová kapacita měla volit rozumně v závislosti na předpokládaném provozu. Zároveň však chceme zajistit co největší možnou přenosovou kapacitu pro méně prioritní toky. Tato metoda je vhodná pro aplikace na přenos hlasu, videa a pro aplikace v reálném čase. A to z důvodu minimálního zpoždění, jeho rozptylu. Zároveň zajišťuje dostatečnou přenosovou kapacitu i pro toky s nižší prioritou [9], [10].

3.2 Parametry kvality služeb

Hlavními parametry QoS, je soubor veličin, podle kterých určujeme celkovou úroveň poskytovaných služeb. Tyto veličiny jsou však velmi závislé na síťovém vybavení trasy mezi zdrojem a cílem. Za účelem poskytnutí co nejlepší kvality služeb je třeba poskytnout tyto parametry co nejlepší.

Mezi hlavní parametry QoS patří:

- přenosová kapacita (bandwidth) [kbit/s],
- ztrátovost paketů (loss rate) [%],
- zpoždění (latency) [ms],
- rozptyl zpoždění (jitter) [ms].

3.2.1 Zpoždění

Zpoždění je doba, za kterou datagram urazí cestu mezi dvěma počítači a zpět. Celkové zpoždění se skládá z několika typů zpoždění, které vznikají na přenosové cestě. Zpoždění snižuje QoS sítě a je pro uživatele nežádoucí. Největší vliv má na služby poskytované v reálném čase kde je zpoždění velmi nežádoucí. Mezi tyto aplikace, poskytované v reálném čase, patří například přenos hlasu a videa. U těchto služeb uživatel již zaregistruje zpoždění větší než 150ms, při hodnotě přesahující 200ms je kvalita přenosu hlasu velmi nízká. Nad 400ms je spojení prakticky nemožné a dá se považovat za nefunkční. Zpoždění se dá také omezit různými metodami snižujícími celkový počet paketů potřebných k přenosu [9], [11].

3.2.2 Ztrátovost paketů

Tato veličina vyjadřuje procentuální počet paketů, které nedorazily do cílové destinace v daném čase, oproti celkovému počtu paketů zaslaných. Datové pakety mohou být ztraceny z různých důvodů, například: zahlcením sítě, nesprávným směrováním, poškozením paketu při odesílání nebo přijímání, přetížením paměti pro jejich dočasné uchování. Také různé druhy rušení mohou pakety po cestě poškodit natolik, že jsou zahozeny.

Pokud dojde k zahlcení sítě tím, že jsou požadovány příliš vysoké přenosové zdroje, uchovávají se pakety v dočasné paměti. Tato paměť není nekonečná a je-li linka obsazená dlouhou dobu, dochází k přetížení paměti a následnému zahazování paketů. Pokud jsou tyto pakety ztraceny, není možné je obnovit, ale je možné požádat o jejich opakované zaslání ze zdroje. To ale způsobuje značnou odezvu a u různých aplikací pracujících v reálném čase je toto řešení zbytečné. Aby se předešlo těmto ztrátám, používá se sledování zatížení sítě a následné řazení do front pomocí metod QoS jako Priority Queuing (PQ) nebo Custom Queuing (CQ). Tyto metody zabráňují přetížení paměti pro dočasné uchování a poskytují prostředky pro včasné odeslání důležitých dat [11], [12].

3.2.3 Rozptyl zpoždění

Rozptyl zpoždění je hodnota, která udává, jaký je rozdíl mezi referenčním časem doručení paketu a reálným časem doručení. Tento rozdíl ať už záporný nebo kladný vyjadřuje kolísání zpoždění při určitém přenosu. Z toho plyne, že by měl být pokud možno nulový. V ideálním případě by pakety měly přicházet bez zpoždění a v konstantních časových intervalech. Avšak reálně dochází k různým zpožděním z důvodu například přetížení sítě nebo změny přenosové cesty. Přípustná velikost rozptylu zpoždění je různá v závislosti na druhu aplikace [12].

3.2.4 Přenosová kapacita

Přenosová kapacita udává přenosovou rychlost, neboli jaký objem dat je daná přenosová cesta schopna přenést za jednotku času. Z toho plyne, že čím větší přenosovou kapacitu můžeme zabezpečit pro přenos, tím větší přenosová rychlost bude. Naopak nedostatečná přenosová kapacita může způsobit zpoždění a po čase i ztrátu paketů při přenosu. Proto je potřeba zvolit přenosovou kapacitu hlavně podle typu komunikace a druhu aplikací, které budou tuto přenosovou cestu využívat. Ačkoli je v dnešní době u většiny přenosových cest přenosová kapacita dostatečná, stále mohou vznikat problémy při přenosu většího množství dat v aplikacích, které požadují větší přenosovou kapacitu [11], [12].

4 METODY ŘÍZENÍ PŘÍSTUPU

Metody řízení přístupu (AC – Admission Control) jsou definovány, jako souhrn akcí, které síť vykoná při vytváření nového spojení a rozhodováním zda toto spojení bude přijaté nebo odmítnuté. Úlohou těchto metod je udržovat rovnováhu mezi dvěma požadavky, a to maximálním využitím síťových prostředků a dodržením daných parametrů spojení. Rozhodovací algoritmus metod AC je první krok při navazování spojení a následným přidělováním síťových zdrojů tomuto spojení. Tento rozhodovací algoritmus musí při přijetí požadavků na nové spojení rozhodnout, zda povolit či zamítnout navázání spojení vzhledem k současnému využití současných síťových zdrojů. Nové spojení je možno navázat pouze pokud jsou dostupné síťové zdroje dostatečné, aby splnili QoS požadavky tohoto spojení a naopak neohrozili QoS žádného z již probíhajících spojení. Pokud tyto dostupné zdroje nejsou dostatečné, pokus o navázání nového spojení je odmítnut.

V současné době existuje velké množství metod AC a jejich modifikací. Některé z těchto metod jsou založeny na různých matematických modelech využívající teorii pravděpodobnosti a statistiky. Dalším druhem metod jsou různé umělé inteligence, tyto přizpůsobivé metody by mohly nahradit současně používané metody, které jsou náročné na výpočtovou kapacitu. Inteligentní metody AC by také byly schopné učit se a předvídat vzniklé situace v síti.

Rozhodovací algoritmus metod AC lze popsat rovnicí [13]

$$P\left(\sum_{i=1}^N r_i(t) \geq C\right) < \varepsilon, \quad (4.1)$$

kde N je počet připojení, $r_i(t)$ aktuální přenosová rychlost, C je celková kapacita linky a ε je ztrátovost paketů .

Základní kritéria AC metod jsou:

- **Jednoduchost** – co nejméně náročná implementace a výpočtová náročnost algoritmu.
- **Rychlost** – rozhodovací algoritmus musí být schopen rozhodovat v reálném čase.
- **Flexibilitnost** – použitý algoritmus by měl být přizpůsobivý k novým typům služeb.
- **Robustnost** – algoritmus metody musí být schopen pracovat efektivně i v případech částečného nebo úplného nedodržení předpokladů.
- **Výkonnost** – algoritmus by měl umožnit využít co největší využití statického multiplexování.
- **Efektivnost** – algoritmus by měl dodržovat garantovanou kvalitu služeb, aby byl použitelný.
- **Řiditelnost** - algoritmus by měl být schopen řídit datový tok bez snížení výkonu sítě [13].

4.1 Difúzní metoda

Tato metoda je založena na posuzování statistické přenosové kapacity na základě porovnávání pomocí modelu difúzní aproximace. Tato difúzní metoda je reprezentována dvěma vztahy pro konečnou (FB – Finite Buffer) a nekonečnou (IB – Infinite Buffer) kapacitou vyrovnávací paměti. V modelu IB je pravděpodobnost ztráty paketu stanovena pomocí pravděpodobnosti přetečení paměti. Tato pravděpodobnost je formulována, jako pravděpodobnost přetečení současné kapacity vyrovnávací paměti K u linky s nekonečně velkou vyrovnávací pamětí kterou můžeme vidět v následující rovnici [14]

$$L_{FB} = \frac{1}{\sqrt{2\pi}} e^{\left\{\frac{2K}{\alpha}(\lambda-C)\right\}} e^{\left\{-\frac{(\lambda-C)^2}{2\sigma^2}\right\}}, \quad (4.2)$$

$$L_{IB} = \sigma L_{FB}. \quad (4.3)$$

Pro N zdrojů, kde zdroj i je charakterizovaný pomocí tří parametrů - R_i vrcholová přenosová rychlost, r_i četnost aktivity zdroje a b_i průměrná délka trvání této aktivity. Mají použité veličiny tento význam:

λ je střední hodnota přenosové rychlosti určená [14]

$$\lambda = \sum_{i=1}^N \lambda_i, \quad (4.4)$$

kde

$$\lambda_i = r_i R_i, \quad (4.5)$$

σ je standartní odchylka přenosové rychlosti určená

$$\sigma^2 = \sum_{i=1}^N \sigma_i^2, \quad (4.6)$$

kde

$$\sigma_i^2 = \lambda_i (R_i - \lambda_i). \quad (4.7)$$

Okamžitá odchylka procesu příjmu paketů α lze vypočítat pomocí vztahu [14]

$$\alpha = \sum_{i=1}^N \lambda_i \frac{1 - (1 - \beta_i T_i)^2}{(\beta_i T_i + \gamma_i T_i)^2}, \quad (4.8)$$

kde hodnota parametru $b_i = \frac{1}{\beta_i}$ označuje střední hodnotu aktivní periody zdroje a $\frac{1}{\gamma_i}$ hodnotu střední neaktivní periody.

Statistická přenosová kapacita je definována jako přenosová kapacita potřebná pro zabezpečení připojení se ztrátou paketů nižší než hodnota ε . Pro dva již zmíněné modely FB a IB získáme statistickou přenosovou kapacitu ze vztahů [14]

$$C_{FB} = \lambda - \delta + \sqrt{\delta^2 - 2\sigma^2\omega_1}, \quad (4.9)$$

$$C_{IB} = \lambda - \delta + \sqrt{\delta^2 - 2\sigma^2\omega_2}, \quad (4.10)$$

kde

$$\delta = \frac{2K}{\alpha} \sigma^2, \quad (4.11)$$

$$\omega_1 = \ln(\varepsilon\sqrt{2\pi}), \quad (4.12)$$

$$\omega_2 = \ln(\varepsilon\lambda\sqrt{2\pi}) - \ln(\sigma). \quad (4.13)$$

Výsledná statistická efektivní přenosová kapacita je určena jako [14]

$$C_{DF} = \max(C_{FB}, C_{IB}). \quad (4.14)$$

Algoritmus rozhodující o přijetí či odmítnutí nového spojení lze shrnout do těchto bodů:

1. sledování hodnot parametrů λ , σ^2 , α po daných časových intervalech,
2. v případě navázání nového připojení se tyto parametry přepočítají, aby zahrnovaly i parametry nového připojení,
3. vypočítává se hodnota C_{DF} ,
4. pokud je splněna podmínka $C_{DF} \leq C$ je nové připojení přijato,
5. pokud není tato podmínka splněna, jsou obnoveny staré parametry a parametry nového připojení vymazány [13], [14].

4.2 Gaussova metoda

Tato metoda slouží k určení požadované přenosové kapacity je poměrně rychlá a jednoduchá. Využívá teorie Gaussova limitního rozdělení, s jejíž pomocí aproximuje rozdělení pravděpodobnosti souhrnného provozu za předpokladu, že počet připojení N se blíží nekonečnu, a žádné těchto připojení nemá výrazně dominantní převahu. Bylo dokázáno, že čím větší je počet připojení, tím více se superpozice blíží Gaussovu modelu. Pokud však počet připojení příliš nízký není tato metoda příliš přesná [13], [15].

Pro odhad celkové přenosové kapacity pak můžeme použít vztah [15]

$$C = \sum_{i=1}^N \lambda_i + a' \sum_{i=1}^N \sigma_i. \quad (4.15)$$

$$a' = \sqrt{-2 \ln \varepsilon - \ln 2\pi}. \quad (4.16)$$

$$\sigma^2 = \frac{1}{N} \sum_{i=1}^N (\lambda_i - \lambda)^2. \quad (4.17)$$

Kde λ je průměrná hodnota přenosové rychlosti, λ_i je přenosová rychlost i -tého zdroje σ je standardní odchylka přenosové rychlosti a N je počet zdrojů.

Analýza Gaussovy metody vede určení pravděpodobnosti přetečení kapacity linky [13]

$$P_{overflow} = P \left[\left(\sum_{i=1}^N r_i(t) \right) \geq C \right] = \frac{1}{\sqrt{2\pi}} e^{-\frac{(\lambda-C)^2}{2\sigma^2}}, \quad (4.18)$$

a k určení horní hranice pravděpodobnosti ztráty paketů

$$P_{overflow} = \frac{E[(\sum_{i=1}^N r_i(t)) - C]^+}{\lambda} \leq \frac{\delta}{\lambda\sqrt{2\pi}} e^{-\frac{(\lambda-C)^2}{2\sigma^2}}. \quad (4.19)$$

4.3 Další metody řízení přístupu

4.3.1 Metody řízení přístupu na základě měření

Metody řízení přístupu na základě měření (MBAC - Measured Based Admission Control) se oproti metodám přístupu založených na parametrech (PBAC - Parameter Based Admission Control) jeví jako efektivnější. Metody MBAC lépe spravují dostupnou přenosovou kapacitu, protože jsou schopné lépe přerozdělovat dostupnou přenosovou kapacitu pro více uživatelů/požadavků. Tato výhoda plyne z toho, že metody MBAC jsou zaměřeny na měření aktuálního zatížení sítě. Nové připojení vyžaduje pouze minimum informací, zbylé informace jsou přímo doplněny měřením. To znamená, že metody MBAC pracují, oproti metodám PBAC, s reálnými hodnotami namísto předdefinovaných konstantních parametrů. Nové připojení je realizováno tak, že počáteční odhad přenosové kapacity je proveden na základě dostupných parametrů a je dále zpřesněn měřením. Z toho plyne, že čím kratší je interval mezi jednotlivými měřeními, tím více připojení může být obslouženo a efektivněji rozdělena přenosová kapacita. Metody MBAC fungují na základě rovnic [16]

$$C_{odhad} = m_{měřené} + p_{nové} + \alpha' \sqrt{\sigma_{měřené}^2}, \quad (4.20)$$

$$(C_{odhad} \times APF) \leq C - \text{akceptováno}, \quad (4.21)$$

$$(C_{odhad} \times APF) > C - \text{zamítnuto}, \quad (4.22)$$

kde C je přenosová kapacita, $m_{měřené}$ je reálná rychlost přenosu všech současných připojení a σ je variace měřených hodnot. Faktor řízení přístupu (APF - Admission Policy Factor) je konstanta, kterou se vyjadřuje přísnost nároků na síť a korigují se s její pomocí nepřesnosti metody [16], [18].

4.3.2 Metody řízení přístupu na základě parametrů

Metody řízení přístupu na základě parametrů (PBAC - Parameter Based Admission Control) jsou často preferovány i přes jejich nižší efektivitu díky snadné implementaci. Také vzhledem k tomu že pracují s parametry pevně danými a neprovádí jejich měření, jsou jejich požadavky na výpočetní kapacitu minimální. Oproti tomu nevýhodou je, že síťové prostředky mohou být rozděleny neadekvátně. Například ve chvíli kdy některém z připojení neprobíhá komunikace, stále zabírá pásmo podle svých parametrů. V takových případech mohou být zamítnuta nová připojení, ačkoli by neovlivňovala kvalitu služeb již aktivních připojení. Tyto metody se dají obecně vyjádřit jako [17]

$$C = m + a'\sigma. \quad (4.23)$$

4.3.3 Algoritmus obyčejného sčítání

Algoritmus obyčejného sčítání (simple-sum – Simple summary) je jedním z nejjednodušších algoritmů AC. Díky tomu je to nejpoužívanější kontrolní algoritmus a v kombinaci s metodou WFQ řazení se často využívá k zajištění co nejnižšího zpoždění. Řídí se podle rovnice [13]

$$C_m + r_{n+1} < C, \quad (4.24)$$

kde C_m je celkový součet již existujících přenosových rychlostí, r_{n+1} je rychlost nového spojení a C je celková kapacita linky [18].

5 NEURONOVÁ SÍŤ

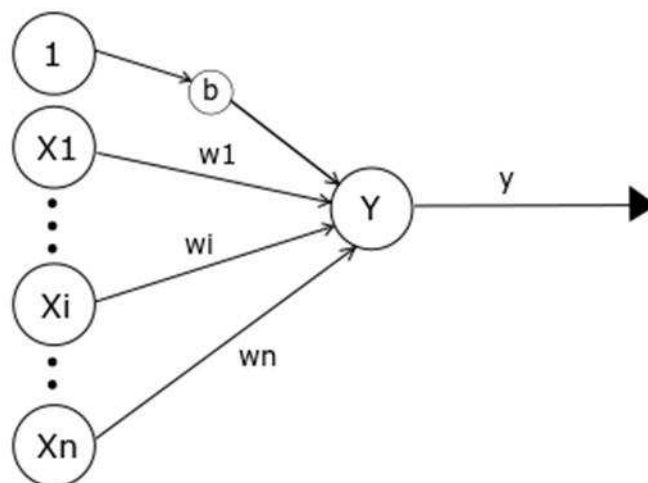
Již od vzniku prvních počítačů se lidé pokoušejí vytvořit algoritmus schopný napodobit lidský mozek, čímž vzniklo odvětví zvané umělá inteligence. Základem umělé inteligence je neuronová síť, což je algoritmus, který se inspiroje biologickou neuronovou sítí. Neuronové sítě se ve dnešní době využívají v řadě analytických a rozhodovacích metodách v různých oborech lidské činnosti. Ve srovnání s ostatními rozhodovacími algoritmy podává extrémně dobré výsledky zejména díky větší rychlosti a dobré schopnosti přizpůsobení se novým podmínkám.

Princip u naprogramované neuronové sítě je podobný, jako u biologické neuronové sítě. Stejně jako v biologické neuronové síti je i zde základním stavebním prvkem nervová buňka - neuron. Jednotlivé neurony jsou vzájemně propojeny a tyto spoje jsou následně ohodnoceny tzv. váhou. Toto vzájemné propojení, schopnost adaptovat se a učit se na základě trénovaných vzorů dává neuronovým sítím velký potenciál v oblasti analýzy dat.

Právě schopnost učit se je největší předností neuronových sítí. Schopností učit se myslíme zapamatovat si kombinace, které vedly k požadovanému výstupu a u nových vstupů pak v závislosti na své paměti odhadovat výsledek. To také umožňuje neuronové síti řešit i silně nelineární úlohy kde selhávají ostatní klasické modely. Nejznámější a nejčastěji používanou metodou učení je algoritmus zpětného šíření chyby (Backpropagation). [7].

5.1 Neuron

Neuron je základní stavební prvek neuronových sítí. Používá se jako nejjednodušší druh neuronové sítě ke klasifikaci lineárně separovatelných vzorů. Každý neuron se skládá ze vstupů opatřených vahami a biasu neuronu.



Obr. 5.1: Model neuronu.

Vnitřní potenciál neuronu reprezentuje suma vážených hodnot vstupů y , kterou lze dopočítat podle vztahu [21]

$$y = bias + \sum_{i=0}^n x_i * w_i, \quad (5.1)$$

kde x_1 až x_n je vektor vstupů, w_1 až w_n vektor vah vstupů a $bias$ představuje doplňkový vstupní neuron s hodnotou +1.

Neuronová síť postavená kolem jediného neuronu, je schopna klasifikace pouze dvou tříd. Rozšířením výstupní vrstvy na více než jeden neuron by bylo možné rozšířit klasifikaci na více tříd. Jednotlivé třídy ale musí být lineárně oddělitelné, aby síť pracovala správně [20].

5.2 Vícevrstvé neuronové sítě

Jednovrstvá neuronová síť je schopna řešit pouze omezenou třídu problémů, a to lineárně separovatelné. Toto omezení bylo považováno za vážný nedostatek. Proto se uvažovalo o přidání dalších (skrytých) neuronů. Avšak vyvstal problém, jakým způsobem by bylo možné adaptovat váhové koeficienty mezi neurony ve skryté vrstvě. Tento problém vyřešil jednoduchý algoritmus, nazývaný metoda zpětného šíření chyby. Díky tomuto řešení se vícevrstvé neuronové sítě staly velmi oblíbené a patří mezi univerzální řešení v různých oblastech informatiky, komunikačních technologií a přírodních věd [19].

5.2.1 Druhy vícevrstevných sítí

I. Hopfieldova neuronová síť

Při studování statistických nelineárních kooperativních systémů, jako například spinové skla, přišli fyzici na myšlenku využít jejich vlastnosti k vytvoření idealizovaných neuronových sítí. Chování těchto systémů je možné přirovnat k mozkovým funkcím, jako je asociativní vyvolávání z paměti nebo zapomínání. Hopfieldovy neuronové sítě se často označují jako autoasociativní neuronové sítě. Patří do třídy buněčných automatů, což jsou dynamické systémy skládající se z velkého množství dvoustavových či vícestavových prvků. Tyto prvky jsou navzájem propojené, s definovanými pravidly na změnu stavu prvků, jejichž makroskopické chování je popsáno analytickými rovnicemi. Tyto autoasociativní sítě jsou jedním z mnoha způsobů vytváření umělých neuronových sítí a modelování mozkových funkcí [19].

II. Rekurentní neuronová síť

Rekurentní neuronová síť se využívá především k analýze posloupností a sekvencí. V tradiční neuronové síti jsou jednotlivé vstupy a výstupy navzájem nezávislé. To však může být nevýhoda, snažíme-li se například odhadnout následující slovo ve větě nebo číslo v řadě na základě předcházejících hodnot. Tyto sítě se nazývají rekurentní, protože provádějí stejné úlohy pro každý prvek sekvence s výsledkem nezávislým na přechozích výpočtech [19].

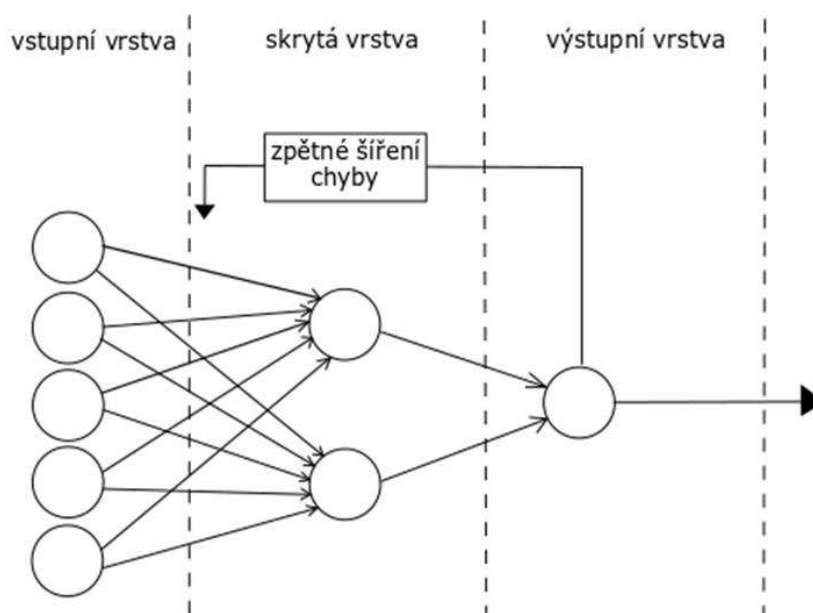
5.2.2 Adaptační algoritmus zpětného šíření chyby

Adaptační algoritmus zpětného šíření chyby, neboli backpropagation, je založen na principu učení se z chyby sítě. Učení se skládá ze dvou průchodů přes vrstvy sítě:

- **Přechod dopředu (forward pass)** – zadají se vstupní proměnné, ty se dál šíří vrstvami sítě. Nakonec jsou vypočítány výstupní hodnoty podle vztahu (5.1) pro všechny vrstvy. Během tohoto průchodu jsou váhy mezi neurony pevné a nemění se.
- **Zpětný přechod (backward pass)** – všechny váhy spojů mezi neurony se přizpůsobí na základě pravidla opravování chyby. Hodnotu chybového signálu E_{total} získáme z rovnice [21]

$$E_{total} = \sum \frac{1}{2} (y_{target} - y_{output})^2, \quad (5.2)$$

kde y_{target} je požadovaná hodnota výstupu a y_{output} je získaná hodnota výstupu. Signál následně postupuje zpětně od výstupní vrstvy ke vstupní. Během tohoto postupu se upravují váhy spojů, aby při příštím přechodu dopředu byly přesnější výsledky [20].



Obr. 5.2: Model změny vah spojů při metodě zpětného šíření chyby.

5.3 Neuronové sítě v AC

Při tradiční metodě analýzy chování sítě ve všech možných situacích pro každý kontrolní bod, je kontrolní mechanismus závislý na analytických výsledcích. Konkrétně na sledovaných parametrech, vypočítaných parametrech a funkci pro určení vhodných kontrolních parametrů provozu pro každou sledovanou situaci, která je definována. Kontrolních mechanismy pro všechny kontrolní body jsou implementovány v síťovém ovladači. Tato metoda způsobuje nejen to, že je tento ovladač velmi komplikovaný, ale také není schopný se rychle přizpůsobit novým změnám v síťovém provozu nebo novým požadavkům. Po každé takovéto změně, je totiž potřeba provést nové simulace a analýzy pro nastalou situaci. Oproti tomu za pomoci „učící se“ kontrolní metody používané v neuronových sítích, můžeme vytvořit ovladač, který se bude automaticky přizpůsobovat nové situaci. Další výhodou neuronové sítě je její schopnost učit se nelineární funkce s velkým množstvím vstupů a výstupů. Toto umožňuje předvídat kvalitu služeb z pozorovaného provozu a následně optimální nastavení kontrolních hodnot. Neuronová síť je také schopna aproximovat komplikované vztahy mezi vstupními a výstupními proměnnými, a to volbou významných vstupů a následném samostatném odvození vlastností parametrů vstupních dat. Tím pádem může ovladač, využívající princip neuronové sítě „učení se“, přesně kontrolovat i takové sítě, které mají proměnné charakteristiky. Tím by do jisté míry mohly neuronové sítě vyřešit optimalizační problémy s přidělováním kapacity spojení. Jsou zde i takové přizpůsobivé kontrolní metody, které nevyužívají neuronových sítí. Avšak tyto metody nemohou zvládnout komplikované nelineární funkce s velkým počtem vstupů a výstupu tak jako neuronové sítě [6].

6 SIMULACE A GRAFY

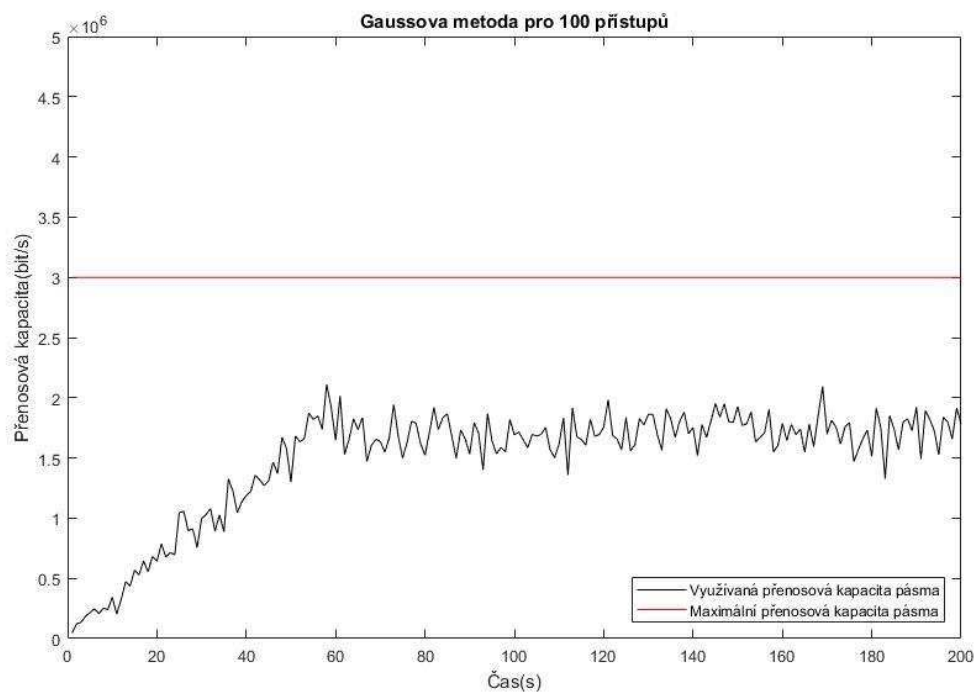
Simulace byly prováděny v programu Matlab, což je interaktivní programové prostředí pro počítání s maticemi, vykreslování 2D i 3D grafů funkcí, implementaci algoritmů, počítačovou simulaci, analýzu a prezentaci dat i vytváření aplikací.

Simulace byly provedeny pro 100, 1 000 a 10 000 přístupů do sítě. Rozhodnutí o přijetí, či zamítnutí přístupu bylo provedeno na základě Gaussovy metody a metody založené na neuronových sítích. Vstupní hodnoty jsou reprezentovány maticí $M \times N$ náhodných hodnot v rozsahu 0 - 64 000 bitů, kde M je počet časových intervalů a N počet přístupů. Tyto náhodné hodnoty představují datový tok kodeku G.711. Časový úsek simulace je 200 sekund rozdělených do časových intervalů. Tyto intervaly jsou 1s pro 100 přístupů, 100ms pro 1 000 přístupů a 10ms pro 10 000 přístupů. Během prvních 100 sekund jsou navazována jednotlivá spojení, pro každý časový interval jeden pokus o spojení. Maximální přenosová kapacita linky byla stanovena na 3Mb pro 100 přístupů, 30Mb pro 1 000 přístupů a 300Mb pro 10 000 přístupů. U neuronové sítě byla hraniční hodnota přenosového kanálu pro přijetí nového připojení stanovena na 95% maximální přenosové kapacity linky.

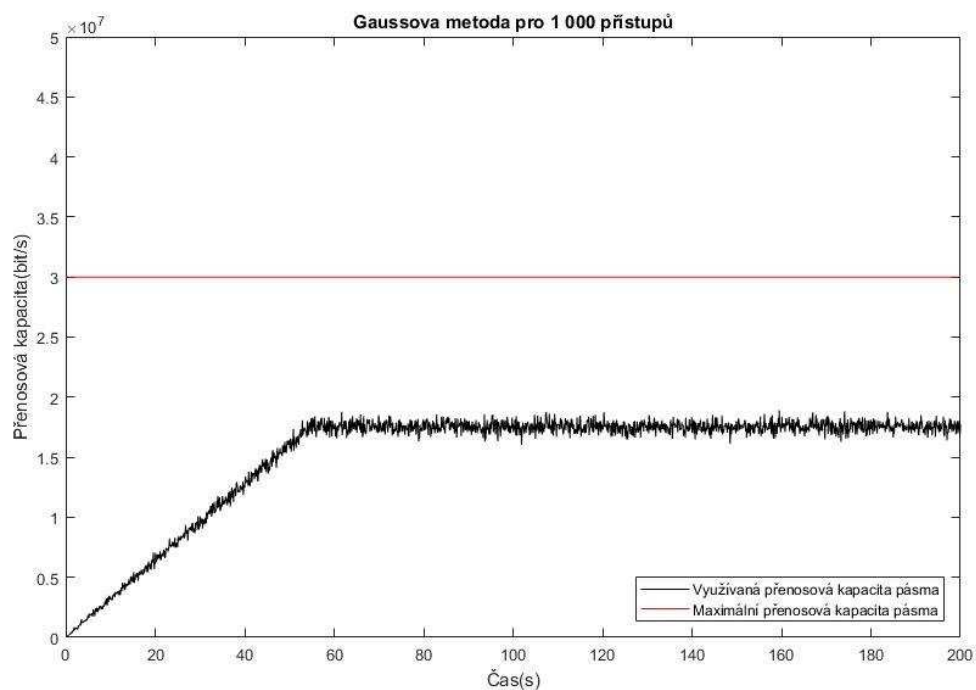
Pro tento typ simulace jsme zvolili neuronovou síť NARNET (Nonlinear autoregressive neural network - nelineární autoregresivní neurální síť) skládající se z 10 skrytých neuronů pro 100, 100 skrytých neuronů pro 1 000 a 200 skrytých neuronů pro 10 000. Odezva sítě byla 2 pro 100, 20 pro 1 000 přístupů a 50 pro 10 000 přístupů. Síť byla vytrénována metodou Levenberg-Marquardt.

6.1 Grafy

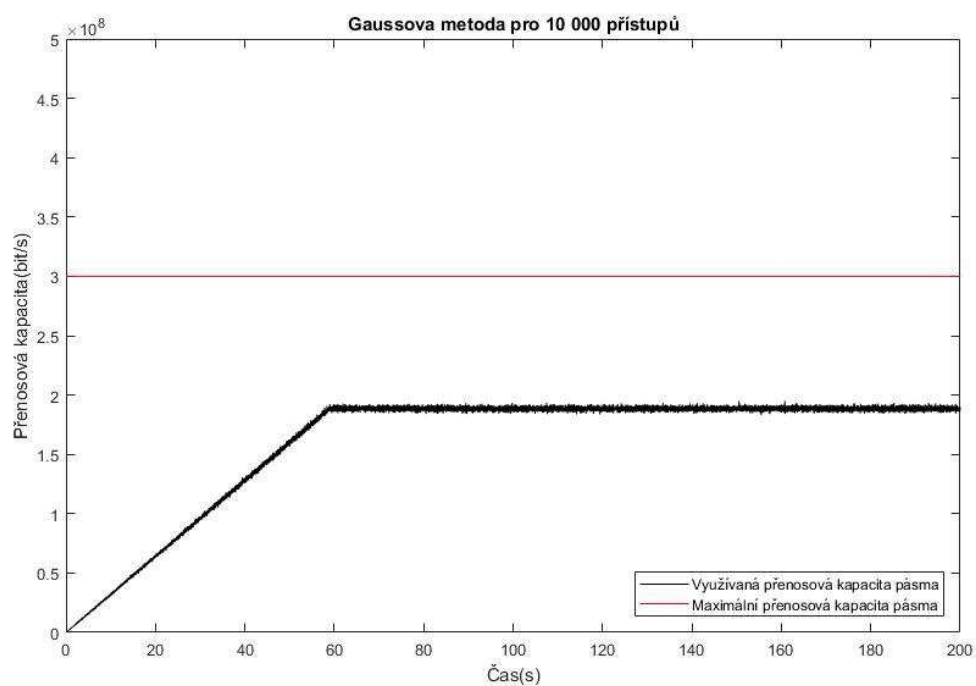
6.1.1 Gaussova metoda



Obr. 6.1: Graf zatížení linky pro Gaussovu metodu se 100 přístupy.

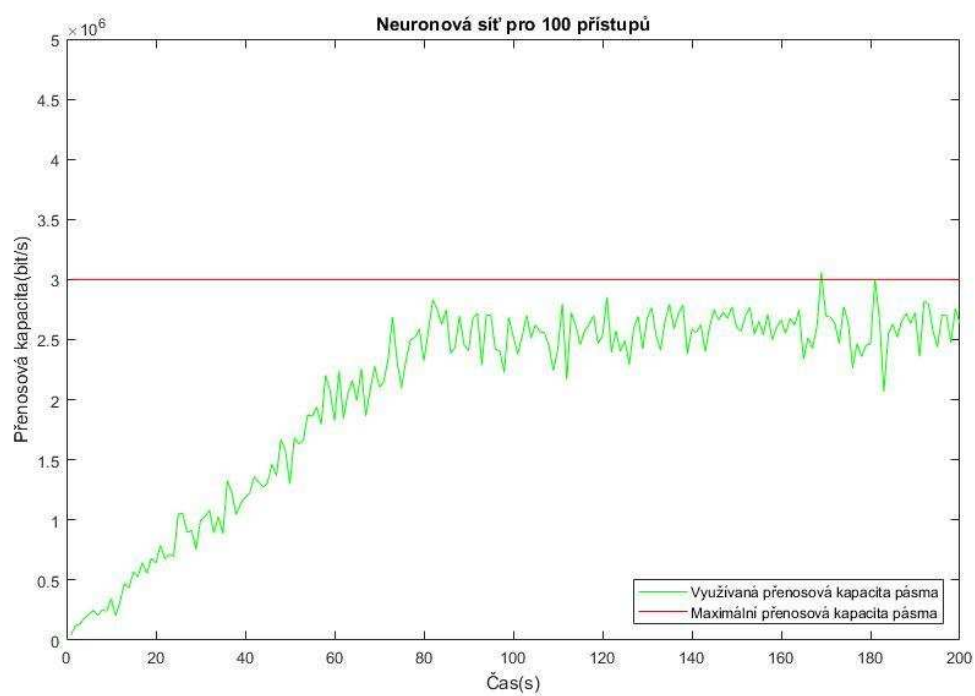


Obr. 6.2: Graf zatížení linky pro Gaussovu metodu se 1 000 přístupy.

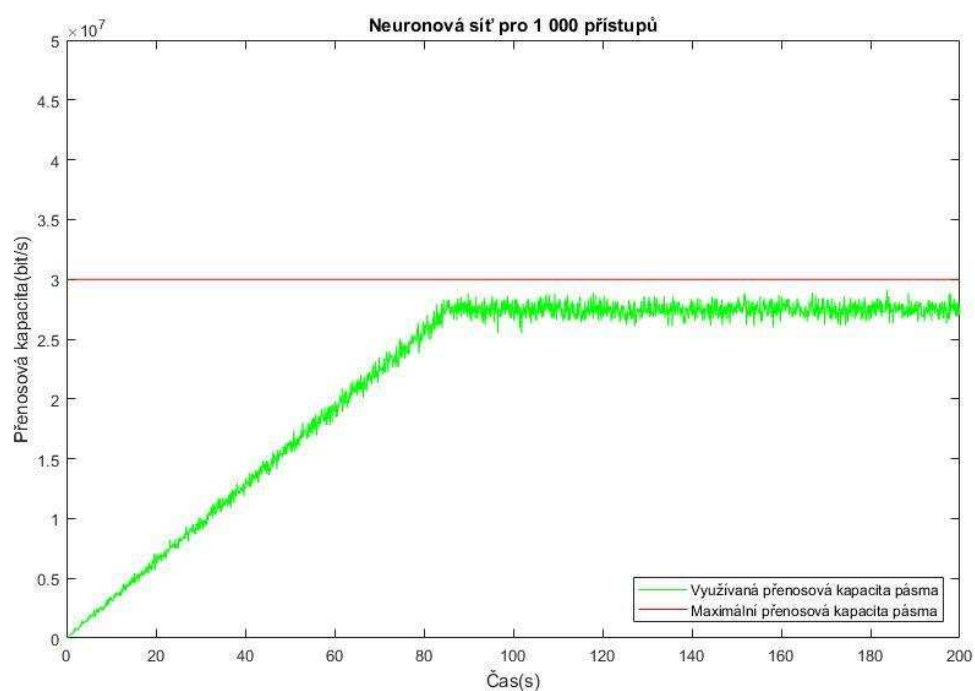


Obr. 6.3: Graf zatížení linky pro Gaussovu metodu se 10 000 přístupy.

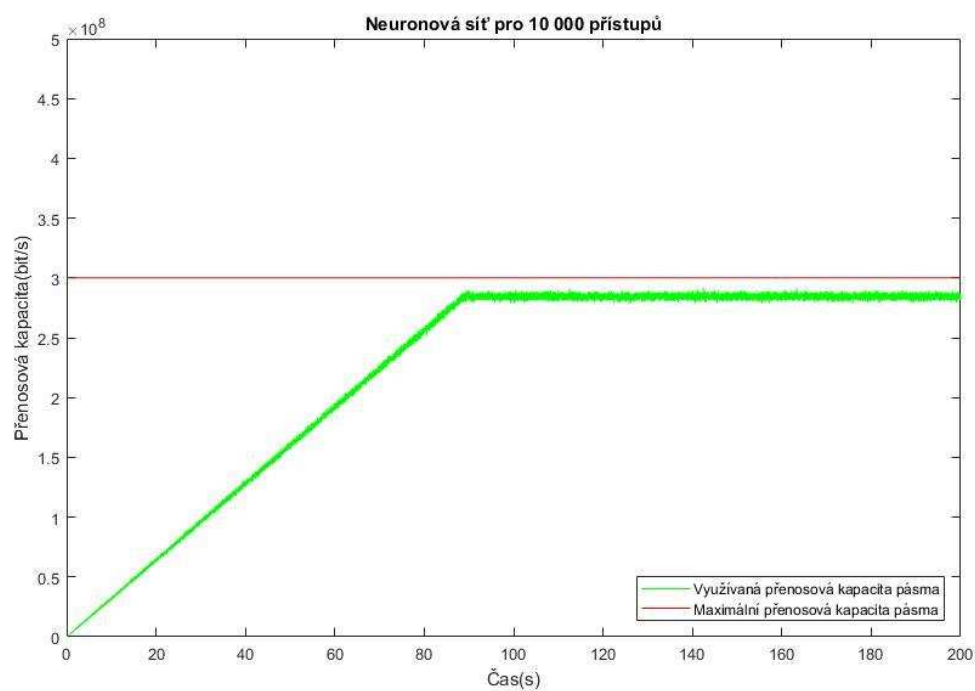
6.1.2 Metoda s neuronovou sítí



Obr. 6.4: Graf zatížení linky pro metodu neuronové sítě se 100 přístupy.

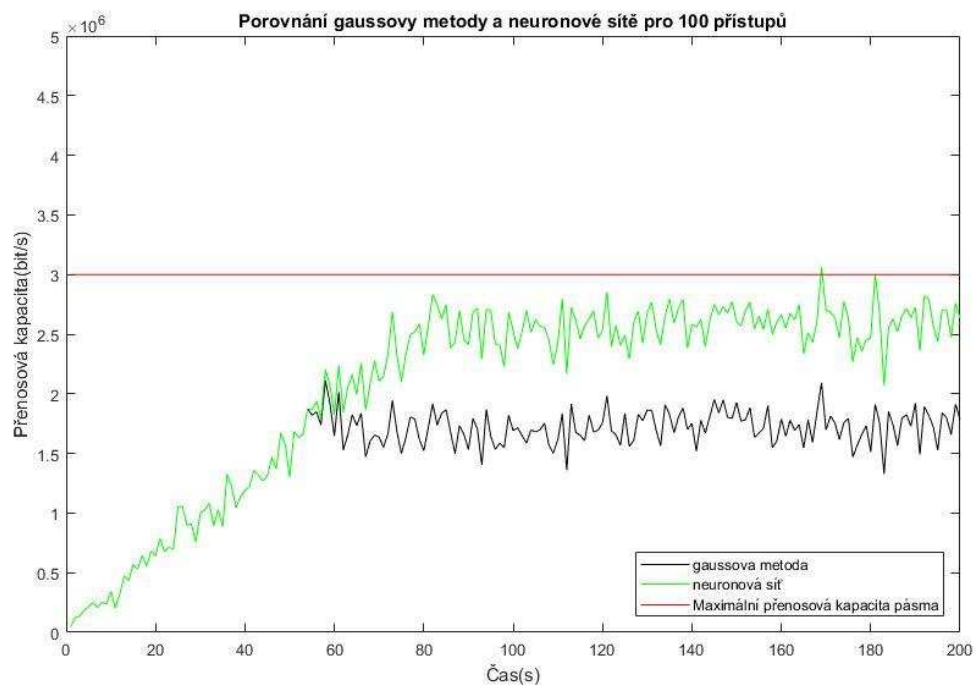


Obr. 6.5: Graf zatížení linky pro metodu neuronové sítě se 1 000 přístupů.

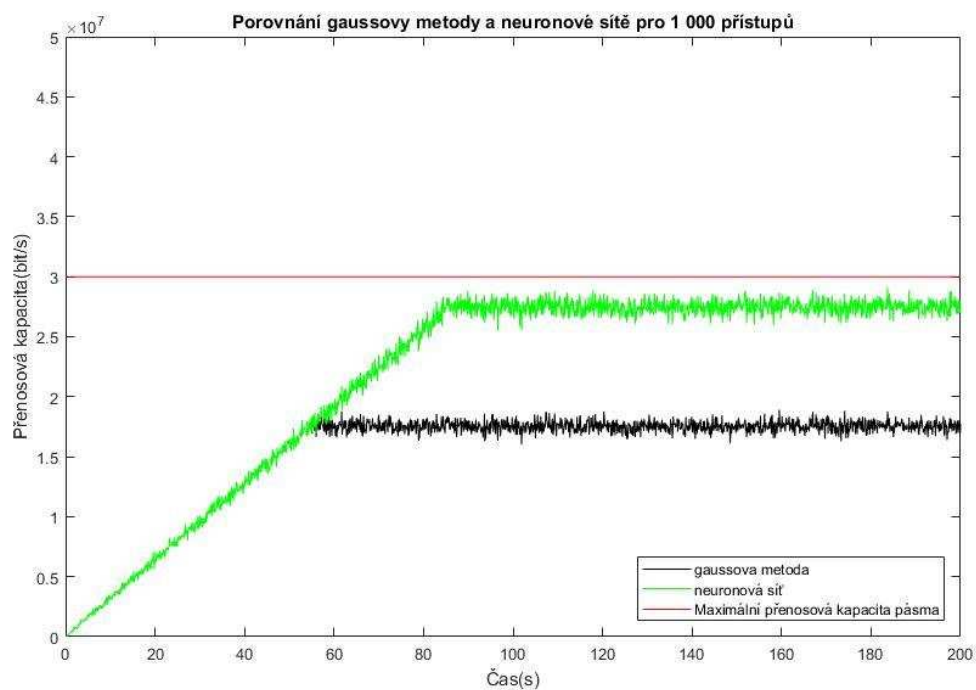


Obr. 6.6: Graf zatížení linky pro metodu neuronové sítě se 10 000 přístupů.

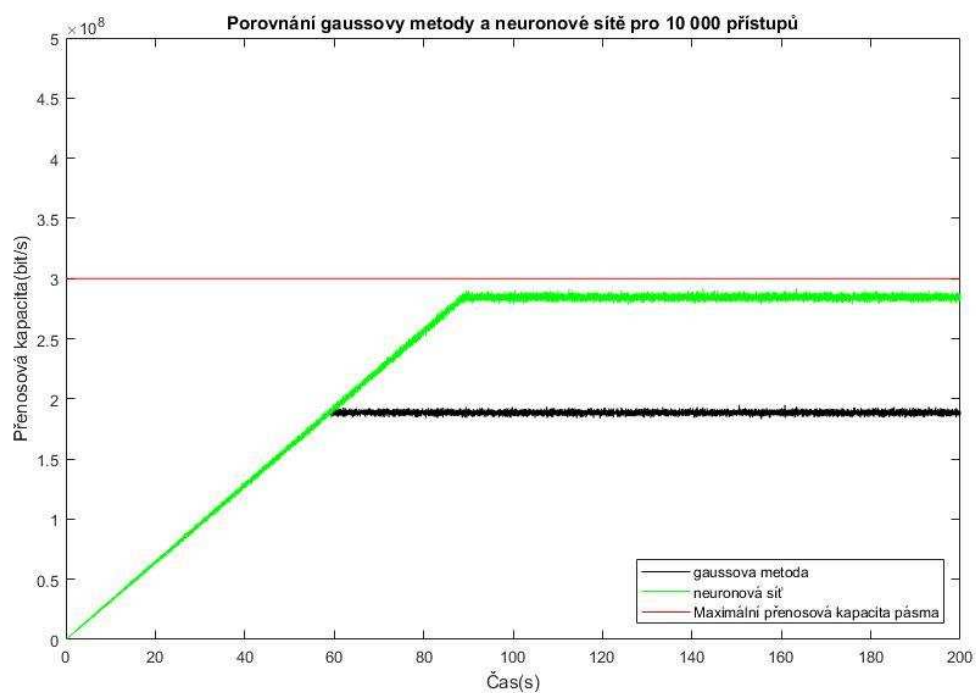
6.1.3 Porovnání



Obr. 6.7: Srovnání zatížení linky pro Gaussovu metodu a neuronovou síť se 100 přístupy.



Obr. 6.8: Srovnání zatížení linky pro Gaussovu metodu a neuronovou síť se 1 000 přístupů.



Obr. 6.9: Srovnání zatížení linky pro Gaussovu metodu a neuronovou síť se 10 000 přístupů.

6.2 Vyhodnocení

Tab. 6.1: Porovnání jednotlivých parametrů pro obě metody.

Metoda	Gaussova			Neuronových sítí		
Počet přístupů	100	1 000	10 000	100	1 000	10 000
Počet povolených přístupů	58	546	5561	84	877	8826

Z grafů je patrné, že metoda využívající neuronovou síť mnohem efektivněji využívá kapacitu přenosové linky. To je dáno především tím, že je schopna mnohem přesněji odhadnout, jak se bude daný datový provoz chovat a podle toho efektivněji rozdělit přenosovou kapacitu mezi jednotlivé zdroje. Na druhou stranu je ale více náchylná k překročení maximální kapacity linky, to by mohlo mít za následek zpoždění paketů nebo jejich případnou ztrátu a tím i snížení kvality služeb. Z tohoto důvodu jsme při simulacích omezili efektivní kapacitu přenosové linky na 95% a 5% celkové přenosové kapacity nechali jako rezervu pro případ přetečení. Tímto krokem jsme sice snížili počet možných připojení, ale zároveň zlepšili kvalitu služeb pro ostatních připojení.

Gaussova metoda se oproti metodě využívající neuronové sítě zdá neefektivní. Vyplývá to zejména ze skutečnosti, že tato metoda je využívána pro svoji jednoduchost a schopnost zajistit požadovanou kvalitu služeb. Metoda počítá pro každý zdroj větší přenosovou kapacitu než je nutné, tím sice značně omezuje efektivitu rozdělení celkové přenosové kapacity, ale je tím zároveň zajištěna požadovaná kvalita služeb i v krajních případech, kdy by například všechny zdroje začaly využívat svoji maximální přenosovou kapacitu ve stejný okamžik.

Ačkoli je Gaussova metoda jednoduchá, je závislá na průběžném přepočítávání parametrů připojení a při větším počtu připojení může tato skutečnost negativně ovlivnit rychlost rozhodování. Na rozdíl od neuronové sítě, která dokáže řešit daný problém víceméně intuitivně bez dlouhých výpočtů. I to je důvod proč pro tuto úlohu vychází neuronová síť jako lepší řešení.

7 ZÁVĚR

Teoretická část této práce obsahovala úvod do problematiky zajištění kvality služeb v IP sítích. Popis různých služeb poskytovaných v sítích IP a jejich požadavky na QoS. Dále práce představuje různé druhy metod pro zajištění této kvality. Specificky se věnuje metodám AC. Popisuje různé druhy těchto metod a to i s využitím neuronové sítě. Právě neuronovým sítím se věnuje poslední teoretická část práce.

V praktické části práce jsme provedli simulaci AC metod pro řízení hlasového provozu. Simulace byla realizována v programu MATLAB. Cílem simulace bylo porovnat efektivitu Gaussovy metody a metody využívající neuronových sítí pro 100, 1 000 a 10 000 přístupů a výsledky interpretovat.

Z výsledků vyplynulo, že Gaussova metoda je výrazně méně efektivní při využití přenosové kapacity kanálu. Naopak je lépe schopna zabránit přetečení kapacity přenosového kanálu a tím zabránit případnému nepříznivému ovlivnění kvality služeb. Výhodou metody využívající neuronové sítě oproti tomu je, že dokáže efektivněji využít přenosové pásmo a povolí více přístupů. Je ale více náchylná k přetečení maximálního kapacity přenosového kanálu.

8 SEZNAM POUŽITÝCH ZKRATEK

AC	Admission Control Řízení přístupu
APF	Admission Policy Factor Faktor řízení přístupu
BES	Best-Effort Service Negarantovaná služba
CQ	Custom Queuing Metoda řazení podle vlastních požadavků
Diffserv	Differentiated Services Diferencované služby
FB	Finite Buffer Omezená vyrovnávací paměť
FIFO	First In First Out Základní metoda řazení paketů „první dovnitř, první ven“
IB	Infinite Buffer Nekonečná vyrovnávací paměť
IMAP	Internet Message Access Protocol internetový protokol pro vzdálený přístup k e-mailové schránce prostřednictvím e-mailového klienta
Intserv	Integrated Service Integrované služby
IP	Internet Protocol Internetový protokol
IPTV	Internet Protocol Television Televizní přenos pomocí protokolu IP
IPv4	Internet Protocol Internetový protokol verze 4
IPv6	Internet Protocol Internetový protokol verze 6

LLQ	Low Latency Queuing Řazení paketů s nízkým zpožděním
MBAC	Measured Based Admission Control Řízení přístupu podle naměřených parametrů
MMO	Massive Multiplayer Online Hra velkého počtu hráčů online
NARNET	Nonlinear autoregressive neural network Nelineární autoregresivní neurální síť
PBAC	Paramater Based Admission Control Řízení přístupu podle daných parametrů
POP	Post Office Protocol Internetový protokol ke stahování emailových zpráv ze serveru.
PQ	Priority Queuing Prioritní řazení
QoS	Quality of Service Kvalita služby
RFC	Request For Document Žádost o dokumenty popisující internetové protokoly
RSVP	Resource ReSerVation Protocol Protokol pro rezervaci síťových prostředků
RTCP	Real-time Transport Control Protocol Řídící protokol RTP
RTP	Real-time Transport Protocol Transportní protokol pro transport v reálném čase
SMTP	Simple Mail Transfer Protocol Internetový protokol určený pro přenos elektronické pošty
TC	Traffic Class Třída provozu
TCP	Transmission Control Protocol Protokol řízení provozu

TOS	Type Of Service Typ služby
UDP	User Datagram Protocol Uživatelský datagramový protokol
URL	Uniform Resource Locator Přesná specifikace umístění
VoD	Video on Demand Video na vyžádání
VoIP	Voice over Internet Protocol Protokol pro přenos hlasu internetový protokolem
WFQ	Weighted Fair Queuing Řazení podle váhy (důležitosti) paketů

9 SEZNAM POUŽITÝCH SYMBOLŮ

α	okamžitá odchylka procesu příjmu paketů
ε	ztrátovost paketů
σ	variance střední hodnoty přenosové rychlosti
λ	střední hodnota přenosové rychlosti
λ_i	střední hodnota přenosové rychlosti i-tého zdroje
b_i	střední hodnotu aktivní doby zdroje
C	Kapacita linky
E_{total}	Hodnota chybového signálu
K	kapacita vyrovnávací paměti
L	pravděpodobnost přetečení
$M_{\text{měřené}}$	reálná rychlost přenosu všech současných připojení
N	Počet přístupů
R_i	špičková hodnota přenosové rychlosti
r_i	střední hodnota přenosové rychlosti
r_{n+1}	přenosová rychlost n+1 zdroje
$R_i(t)$	okamžitá přenosová rychlost i-tého zdroje
w_i	váha i-tého vstupu
x_i	hodnota i-tého vstupu
y_i	hodnota výstupu

10 SEZNAM POUŽITÝCH ZDROJŮ

- [1] CERF, Vinton G. a Robert E. ICAHN. A protocol for packet network intercommunication. ACM SIGCOMM Computer Communication Review. 2005, **35**(2), 71-. DOI: 10.1145/1064413.1064423. ISSN 01464833. Dostupné také z: <http://portal.acm.org/citation.cfm?doid=1064413.1064423>
- [2] BALEJ J. *Simulace QoS v nástroji Network Simulator*. Brno: Vysoké učení technické v Brně. Fakulta elektrotechniky a komunikačních technologií. Ústav telekomunikací, 2008. 58 s., Vedoucí práce bakalářské práce Ing. Milan Šimek.
- [3] NOVOTNÝ, Vít. *Požadavky různých druhů provozu na kvalitu služby*. Laboratorní úloha. Brno: FEKT VUT v Brně.
- [4] XIAO, Yang, Xiaojiang DU, Jingyuan ZHANG, Fei HU a Sghaier GUIZANI. Internet Protocol Television (IPTV): The Killer Application for the Next-Generation Internet. IEEE Communications Magazine [online]. 2007, **45**(11), 126-134 [cit. 2017-05-29]. DOI: 10.1109/MCOM.2007.4378332. ISSN 0163-6804. Dostupné z: <http://ieeexplore.ieee.org/document/4378332/>
- [5] GOODE, B. Voice over Internet protocol (VoIP). Proceedings of the IEEE [online]. 2002, **90**(9), 1495-1517 [cit. 2017-05-29]. DOI: 10.1109/JPROC.2002.802005. ISSN 0018-9219. Dostupné z: <http://ieeexplore.ieee.org/document/1041060/>
- [6] HIRAMATSU, A. ATM communications network control by neural networks. IEEE Transactions on Neural Networks [online]. **1**(1), 122-130 [cit. 2017-05-30]. DOI: 10.1109/72.80211. ISSN 10459227. Dostupné z: <http://ieeexplore.ieee.org/document/80211/>
- [7] ULDRICH, Miloš a Tomáš. Neuronové sítě a jejich využití. IT Systems [online]. **3**(2014), 3 [cit. 2017-05-30]. Dostupné z: http://www.statsoft.cz/file1/PDF/Statsoft_neuronove_site.pdf

- [8] DYE, Mark A., Rick. MCDONALD a Antoon W. RUFI. Network fundamentals: CCNA exploration companion guide. Indianapolis, c2008. ISBN 978-1-58713-208-7.

- [9] Ing. Michal Halás, PhD. : VoIP – *technické a kvalitatívne aspekty* Prezentace Neverejné telekomunikačné siete a služby, Fakulta elektrotechniky a informatiky, Slovenské technická univerzita v Bratislave, Ústav telekomunikácií.

- [10] KUMAR, Ajith; THORENOOR, S. Ganesh. Analysis of IP Network for different Quality of Service. In: International Symposium on Computing, Communication, and Control (ISCCC 2009) Proc. of CSIT. 2011.

- [11] Advanced VoIP. VoIP QoS. Version 1.0 of 2006-09-04.
URL: <http://www.advancedvoip.com/whitepapers/VoIP%20QoS.pdf>

- [12] RADMAND, Pedram a Alex TALEVSKI. Impact of Encryption on Qos in Voip. 2010 IEEE Second International Conference on Social Computing [online]. IEEE, 2010, , 721-726 [cit. 2017-05-29]. DOI: 10.1109/SocialCom.2010.112. ISBN 978-1-4244-8439-3. Dostupné z: <http://ieeexplore.ieee.org/document/5591496/>

- [13] Ing.Trška R. *Kvalita služieb v ATM*. Bratislava: Slovenská technická univerzita, Fakulta elektrotechniky a informatiky, 2008. 133 s. Vedoucí prof. Ing. Ivan Baroňák, CSc.

- [14] Kavacký M., Baroňák I., "EVALUATION OF TWO STATISTICAL CAC METHODS FOR VARIABLE BIT RATE TRAFFIC SOURCES." In: Journal of ELECTRICAL ENGINEERING, VOL. 59, NO. 4, 2008, 178-186, URL: http://iris.elf.stuba.sk/JEEEC/data/pdf/4_108-02.pdf

- [15] Trška R., Baroňák I., Kvačkaj P., "CAC – CONNECTION ADMISSION CONTROL IN ATM NETWORKS" In: Journal of ELECTRICAL ENGINEERING, VOL. 56, NO. 5-6, 2005, 162–164, URL:
http://iris.elf.stuba.sk/JEEEC/data/pdf/05-06_105-09.pdf

- [16] ADF92 Mičuch, Juraj - Baroňák, Ivan: Preventívne metódy zabezpečenia kvality služby v IP sieťach. In: EE časopis pre elektrotechniku a energetiku. - ISSN 1335-2547. - Roč. 15, mimoriadne č (2009), s. 133-137 URL:
<http://www.posterus.sk/?p=7139>

- [17] CHROMY, Erik, Marcel JADRON a Tomas BEHUL. Admission Control Methods in IP Networks. Advances in Multimedia [online]. 2013, **2013**, 1-7 [cit. 2017-05-29]. DOI: 10.1155/2013/918930. ISSN 1687-5680. Dostupné z:
<http://www.hindawi.com/journals/am/2013/918930/>

- [18] Georgoulas, S, Trimintzios, P, Pavlou, G and Ho, KH (2005) Measurement-based Admission Control for Real-time Traffic in IP Differentiated Services Networks In: IEEE ICT 2005, 2005-05-03 - 2005-05-06, Cape Town, South Africa. URL:
<https://www.ee.ucl.ac.uk/~gpavlou/Publications/Conference-papers/Georg-05a.pdf>

- [19] KVASNIČKA, Vladimír. *Úvod do teórie neurónových sietí*. Slovenská republika: IRIS, 1997. ISBN 80-887-7830-1.

- [20] HAYKIN, Simon. Neural networks: a comprehensive foundation. 2nd ed. Delhi: Pearson Education, 1999. ISBN 81-780-8300-0.

- [21] VOLNÁ, Eva. *Neurovnové sítě I*. Ostravská univerzita v Ostravě, 2008.